

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. NAGEL
CLERK OF COURT

2020 JAN -2 AM 10: 08

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTON
3:20mj003In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH APPLE ID
shawn.walton465@icloud.com STORED AT PREMISES
CONTROLLED BY APPLE, INC.

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

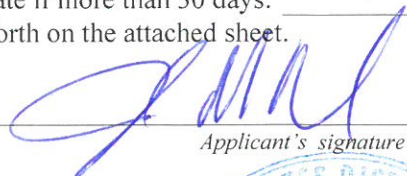
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 USC §§ 846 and 841(a)(1)	Possession with the intent to distribute and to distribute a controlled substance and conspiracy to commit the same
21 USC §843(b)	Use of a communications facility to commit a crime

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



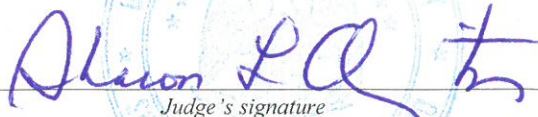
Applicant's signature

Special Agent Joseph Reder, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date:

1-2-20



Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U.S. Magistrate
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
APPLE ID shawn.walton465@icloud.com
THAT IS STORED AT PREMISES
CONTROLLED BY APPLE, INC.

Case No. **3:20mj003**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, JOSEPH M. REDER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Drug Enforcement Administration (DEA) and have been since January 2006. I have completed basic law enforcement training at the DEA Academy in Quantico, Virginia and have received extensive training in the investigation of offenses involving controlled substances. For the past 14 years, I have been assigned to the DEA Cincinnati Resident Office, working on complex conspiracy investigations. During that time, I have participated in multiple investigations, as the case agent and assisting other agents. During that time, I have further had the opportunity to interview drug users and drug traffickers and

become familiar with the various techniques employed by these subjects to use, distribute, and transport narcotics. On October 31, 2016, I was assigned as a Task Force Officer to the Hamilton County Heroin Task Force and on November 9, 2016, I was sworn in as a Deputy Sheriff with the Hamilton County Sheriff's Office in Cincinnati, Ohio. I spent approximately 18 months on the Heroin Task Force and in that time worked on numerous drug overdose death investigations associated with methamphetamine, heroin, cocaine, fentanyl, carfentanil and other illicit narcotics.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, contraband, instrumentalities, and/or fruits of violations of 21 U.S.C. §§ 846 and 841 (possession with the intent to distribute and to distribute a controlled substance and conspiracy to commit the same); and 21 U.S.C. § 843(b) (use of a communications facility to commit a felony), as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The United States, including the DEA, is conducting a criminal investigation of the WALTON Drug Trafficking Organization regarding possible violations of 21 U.S.C. §§ 846 and 841 (possession with the intent to distribute and to distribute a controlled substance and conspiracy to commit the same); and 21 U.S.C. § 843(b) (use of a communications facility to commit a felony).

7. I have personally participated in this investigation and have spoken to, as well as received information from, other agents and investigators participating in this matter. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. The WALTON Drug Trafficking Organization (DTO) is led by ROGER WALTON, originally from Dayton, Ohio. ROGER WALTON'S brother, SHAWN WALTON is a prominent member of the DTO. The WALTON DTO traffics in multi-kilogram quantities of fentanyl, cocaine, and marijuana. Several years ago, ROGER WALTON and his brother SHAWN WALTON relocated from Dayton, Ohio to the greater-Charlotte, North Carolina area to continue and expand their drug trafficking activity. Your affiant submits, based on the facts below, that there is probable cause to believe that SHAWN WALTON uses shawn.walton465@icloud.com to communicate concerning narcotics trafficking and that information concerning narcotics trafficking will be stored at this address.

9. According to cooperating defendant #1 (CD-1) and cooperating defendant #2 (CD-2),¹ the WALTON DTO obtains multi-kilogram quantities of fentanyl, cocaine, and marijuana from suppliers based in the Los Angeles, California and south Texas area. SHAWN WALTON coordinates and facilitates the purchase and sale of wholesale quantities of fentanyl, cocaine, and marijuana. SHAWN WALTON showed CD-1 a kilogram of cocaine at a car wash belonging to the WALTON DTO in the Summer of 2017.

10. The WALTON DTO appears to use trusted associates, including Dayton natives, to transport the narcotics from Texas and California to Charlotte, North Carolina. For example, on August 9, 2018, Oklahoma State Troopers stopped Nathan Scott GODDARD, Jr. (detained), a Dayton resident, and Leyton Wint driving a Dodge Caravan on Interstate 40 in Oklahoma City, Oklahoma. Inside a hidden aftermarket compartment in the Dodge Caravan, Oklahoma State Troopers recovered approximately nineteen kilograms of cocaine. License plate readers showed the Dodge Caravan had made nine trips from the East Coast to the West Coast in the previous six months.

11. Upon the arrival of the narcotics in Charlotte, the WALTON DTO divies up the narcotics according to CD-1 and CD-2. The WALTON DTO sells cocaine and marijuana in the greater-Charlotte area according to CD-1. The WALTON DTO, also sends multi-kilogram amounts of cocaine and fentanyl to Dayton, Ohio. On November 4, 2019, law enforcement served a search warrant on a residence used by GODDARD to store and distribute multi-kilogram quantities of cocaine and fentanyl in Dayton, Ohio. GODDARD was present at the time of the

¹ Cooperating Defendant #1 and #2 are providing information for consideration as to charges and possible sentence related to drug trafficking.

initial execution of the search warrant. Law enforcement officers located and seized pounds of marijuana, more than six kilograms of cocaine, more than four kilograms of fentanyl, and three firearms, and over \$40,000 in cash. Fourteen cellular telephones were recovered, including a cellular telephone assigned telephone number (937) 715-2995 and a cellular telephone assigned telephone number (704) 492-3241.

12. It appears that SHAWN WALTON collects bulk cash from the sale of narcotics. In August 2017, a Charlotte/Mecklenberg police officer, conducted a routine stop of SHAWN WALTON. WALTON had marijuana and over \$30,000 in cash in his possession. WALTON claimed the money was proceeds from a night club. On January 18, 2018, a search warrant of SHAWN WALTON's residence in Charlotte, North Carolina yielded a small amount of marijuana and \$185,324 in cash (mostly \$100 and \$50 notes).

13. SHAWN WALTON appears to use telephone number (704) 497-1615. On December 11, 2019, investigators served AT&T with administrative subpoena requesting subscriber information and call detail records for telephone number (704) 497-1615. AT&T responded that telephone number (704) 497-1615 was activated on April 6, 2018 and subscribed to by SHAWN WALTON at 5656 Tipperlinn Way, Charlotte, NC 28278.

14. Toll record analysis shows that SHAWN WALTON using (704) 497-1615 contacted (937) 715-2995 believe to be used by Nathan GODDARD (and discovered during the Nov. 4, 2019 search warrant described above) ninety-two times between August 24, 2019 and

October 29, 2019. Toll records also showed that SHAWN WALTON using (704) 497-1615 contacted (937) 715-2995 four times on October 29, 2019.²

15. Further analysis of call detail records for (704) 497-1615 believe to be used by SHAWN WALTON show seventeen contacts with (704) 281-9664 between November 12 and December 3, 2019. Investigators previously have identified telephone number (704) 281-9664 as being used by Glynn Sewell, aka “Frezzy.” A former cooperating defendant (CD-4) identified Sewell as a heroin distributor in the Charlotte, North Carolina area. Further, based on conversations CD-4 had with Sewell, Sewell was part of a drug trafficking organization with significant ties to Ohio. CD-4 had numerous conversations with Sewell regarding purchasing heroin from Sewell however, before any purchases were made, CD-4 was incarcerated in North Carolina as a result of a pending drug charge.

16. In mid-December, investigators served Apple, Inc. with an administrative subpoena. Apple, Inc. responded that telephone number (704) 497-1615 was tied to an iCloud account with apple id shawn.walton465@icloud.com. This account was created on August 15, 2019. The iCloud includes bookmarks, contacts, iCloud Backup, iCloud Drive, iCloud photos,

² Cooperating Defendant #3 (hereinafter CD-3)² informed law enforcement that s/he had direct knowledge through previous conversations with GODDARD that Roger WALTON supplied GODDARD with fentanyl and cocaine in Dayton, Ohio. CD-3 stated that he/she had obtained approximately one pound of marijuana from Goddard on or about November 3, 2019. CD-3 stated that this transaction occurred in the basement of 1454 Ruskin Road, Dayton, Ohio. CD-3 stated that during this transaction CD-3 observed approximately ten kilograms of drugs in the basement of 1454 Ruskin Road, Dayton, Ohio. CD-3 stated that Goddard purported the drugs to be fentanyl.

CD-3 had saved telephone number (704) 492-3241 as “Nate” in his telephone. CD-3 stated Nathan Goddard used this telephone number.

mail, and notes. There are FaceTime communications, iCloud communications. Apple, Inc. also responded that telephone number (704) 497-1615 was tied to an iCloud account with apple id shawnwalton495@gmail.com. This account was created on May 18, 2018. This iCloud account has bookmarks and Find My Friends.

17. Based on training and experience, your affiant knows that drug traffickers frequently use wireless/cellular telephones to carry out their activities. Drug dealers use cellular telephones to communicate with customers, their associates and their suppliers. It is often common for drug traffickers to have multiple telephones because certain phones made be used only for certain purposes. For instance, a trafficker may use one telephone just to speak to his supplier, while using a different phone to speak only to his customers. This is a counter-surveillance technique intended to make it harder for law enforcement to identify the user of the phones and his associates.

18. Your Affiant also knows that traffickers commonly text message, each other or their customers, such as meeting locations, prices, and other information needed to carry out the sale of drugs (sometimes in code) and do so using cellular telephones and smart phones. Your affiant also knows that narcotics traffickers also frequently communicate with each other via iMessage, FaceTime, Whats App, and other application further their drug trafficking activities. In these communications, drug traffickers discuss the price, quantity, and availability of narcotics as well as the distribution of narcotics. Drug traffickers also coordinate the shipment of narcotics from source locations to distribution locations. Drug traffickers also relay how to collect payment for the purchase of these narcotics. Drug traffickers often use iMessage, FaceTime, and Whats App because they can be difficult for law enforcement to intercept.

19. Drug traffickers commonly store phone numbers for their associates and customers in the electronic phone book/contacts list, often under alias or code names. Your affiant knows that traffickers, using digital cameras located on their cellular phone or other electronic devices, will sometimes use these devices to take photographs or videos of themselves, their location, their product, their firearms or their associates, which can be electronically stored on and transmitted from these electronic devices. Information can also be downloaded from the internet onto the cellular phone or smart devices, such as email, social network information (like "Facebook"), travel information like maps or directions or photographs. Call data, Facetime, iMessaging, are often electronically stored in the cellular phone. This information can be evidence of who possessed or used a cellular phone at a given time, can contain direct evidence of drug trafficking acts, and can help identify drug trafficking locations or associates through GPS data. I also know that drug dealers use applications on Smart Phones or Devices such as an iPad to communicate in the manner described above with customers, suppliers and associates.

20. In this modern era, individuals also use smart telephones and smart devices to logon to online banking platforms. I know that drug traffickers often use banking services to transmit money to their domestic and international suppliers.

21. Based on my training and experience, your affiant knows that information, such as text messages, photographs, communication applications, contact lists, banking applications, locations, can be saved to the iCloud.

INFORMATION REGARDING APPLE ID AND iCloud³

22. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

23. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

³ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or

through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

24. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

25. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

26. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the

length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

27. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

28. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be

captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

29. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

30. This is a narcotics investigation into the WALTON DTO. SHAWN WALTON contacts Nathan Goddard as well as Glynn Sewell. Investigators have learned that the WALTON DTO supplies both Goddard and Sewell with drugs. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal

activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

31. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

32. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

33. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

34. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

35. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant.

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

39. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

/

/

/

/

/

/

/

/

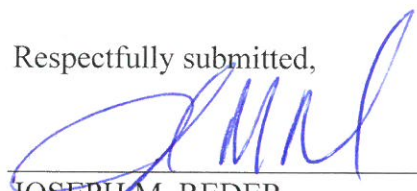
/

/

REQUEST FOR SEALING

40. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

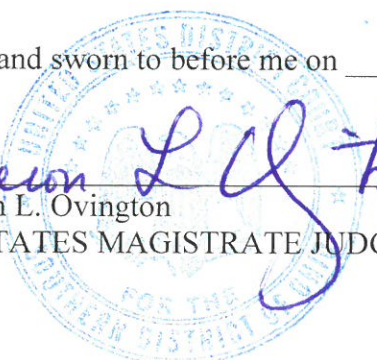


JOSEPH M. REDER
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me on January 2, 2020



Hon. Sharon L. Ovington
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple ID shawn.walton465@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber

Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from May 18, 2018, up to and including the date that Apple, Inc. furnishes the requested information to the government, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account May 18, 2018, up to and including the date that Apple, Inc. furnishes the requested information to the government, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 21 U.S.C. §§ 846 and 841 (possession with the intent to distribute and to distribute a controlled substance and conspiracy to commit the same); and 21 U.S.C. § 843(b) (use of a communications facility to commit a felony) involving ROGER WALTON, SHAWN WALTON, NATHAN GODDARD, and other co-conspirators from May 18, 2018, up to and including the date that Apple, Inc. furnishes the requested information to the government, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The sale and distribution of cocaine and fentanyl and receipt of money for such purchases
- b. Communications between Roger Walton, Shawn Walton, Nathan Goddard and other co-conspirators
- c. Lists of customers and related identifying information;
- d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- e. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- f. All bank records, checks, credit card bills, account information, and other financial records;
- g. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

- h. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- i. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- j. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- k. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.